5

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/862,801 | 05/22/2001 | Vitaly Neyman | 655/63958 | 1154 |

7590 08/01/2005

RICHARD F. JAWORSKI
Cooper & Dunham LLP
1185 Avenue of the Americas
New York, NY 10036

| EXAMINER | |
|---|---|
| ZAND, KAMBIZ | |
| **ART UNIT** | **PAPER NUMBER** |
| 2132 | |

DATE MAILED: 08/01/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

8

| | | | |
|---|---|---|---|
| ***Office Action Summary*** | **Application No.**<br>09/862,801 | **Applicant(s)**<br>NEYMAN ET AL. | |
| | **Examiner**<br>Kambiz Zand | **Art Unit**<br>2132 | |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on 27 June 2005.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) 1-32 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-32 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Kambiz Zand

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

RD

## DETAILED ACTION

1. The text of those sections of Title 35,U.S.Code not included in this section can be found in the prior office action.
2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
3. Claims 1-32 are pending.
4. Examiner withdraws objection of claim 3 due to typo error by the Examiner.

### *Response to Arguments*

5. Applicant's arguments filed 06/27/2005 have been fully considered but they are not persuasive.

As per Applicant's arguments that "the office action refers to page 1 and 2 of the specification as allegedly disclosing admitted prior art. In response, applicants respectfully point out that the portion of the specification referred to in the office action is actually "related Art" No admission, express or implied, has been made that any description in the specification is "prior art" to the present disclosure within the meaning of the patent statues", Examiner refers Applicants to the following remarks:

- Description of the Related Art including information disclosed under CFR 1.97 and 37 CFR 1.98 also may be titled as "Background Art" See MPEP 608.01(c).

- It is defined as "related art known to the applicant" and including "problems involved in the prior art which are solved by Applicant's invention".
- Page 1 and 2 of the specification only describe heuristic detection methods that are well known prior art.

Therefore applicant's above arguments are not persuasive based on the above remarks.

However examiner would reconsider if Applicant provides explicit answer to the following questions since the disclosure is silence in that regard:

a) **What are the problems involved in the Prior Art, which are solved by Applicant's invention**?

b) **How does Applicant's invention overcome the deficiencies of the Prior Art**?

### *Claim Rejections - 35 USC § 103*

6. **Claims 1-32** are rejected under 35 U.S.C. 103(a) as being unpatentable over Joyce (6,519,703 B1) in view of Applicant Admittance Prior Art (AAPA).

**As per claims 1, 7, 13 and 19** Joyce (6,519,703 B1) teach a method, system, storage medium and a programmed computer system including computer executable code for selecting a detection method for analyzing computer code for malicious code (see abstract; fig.2 and associated text), comprising: providing a plurality of malicious code detection methods (see abstract; col.2, lines 16-29); determining a probability of accuracy of a result of the analysis (see abstract; col.2) , and repeating the analyzing and determining steps, if the probability of accuracy is below a predetermined level (see abstract; col.2, lines 42-65 where the assigned confidence rating corresponds to Applicant's predetermined level; col.2, lines 53-57 where if it is a poor confidence which corresponds to Applicant's below pre determined level); and outputting a result of the analysis if the probability of accuracy is at or above the predetermined level (see col.2, lines 47-51 where if it is a high confidence which corresponds to Applicant's at or above pre-determined level), also see col.2-6 and col.7, lines 1-5 for more detailed but do not disclose explicitly wherein at least some of the malicious code detection methods require different amounts of time to analyze for malicious code; selecting a fastest one of the malicious code detection methods, analyzing computer code for malicious code using the selected malicious code detection method; selecting a next fastest one of the malicious code detection methods. However AAPA disclose at least some of the malicious code detection methods require different amounts of time to analyze for malicious code; selecting a fastest one of the malicious code detection methods, analyzing computer code for malicious code using the selected malicious code detection method; selecting a next fastest one of the malicious code detection methods (see page 1 and 2 of the specification). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize AAPA's prior art disclosure in Joyce's Heuristic's packet filtering analysis in order to provide different methods based on Heuristic's logic based rules.

**As per claims 2, 8, 14 and 20** Joyce (6,519,703 B1) teach the method, system, storage medium including computer executable code for selecting a detection method as recited in claims 1, 7, 13 and 19, wherein at least some of the malicious code detecting methods use heuristic logic to detect for malicious code (see abstract; col.2).

**As per claims 3, 9, 15 and 21** Joyce (6,519,703 B1) teach the method, system, storage medium including computer executable code for selecting a detection method as recited in claims 1, 7, 13 and 19 as applied above but do not explicitly disclose, wherein the fastest one of the malicious code detecting methods is a least accurate one of the plurality of malicious code. However AAPA disclose wherein the fastest one of the malicious code detecting methods is a least accurate one of the plurality of malicious code (see page 2, last paragraph of the specification). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize AAPA's prior art disclosure in Joyce's Heuristic's packet filtering analysis in order to provide different methods based on Heuristic's logic based rules.

**As per claims 4, 10, 16 and 22** Joyce (6,519,703 B1) teach the method, system, storage medium including computer executable code of selecting a detecting method as recited in the claims 1, 7, 13 and 19 as applied above but do not explicitly disclose, wherein the slowest one of the malicious code detecting methods is a most accurate one of the plurality of malicious code. However AAPA disclose wherein the slowest one of the malicious code detecting methods is a most accurate one of the plurality of malicious code (see page 2, last paragraph of the specification). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize AAPA's prior art disclosure in Joyce's Heuristic's packet filtering analysis in order to provide different methods based on Heuristic's logic based rules.

**As per claims 5, 11, 17 and 23** Joyce (6,519,703 B1) teach the method, system of selecting a detecting method as recited in the claims 1, 7, 13 and 19, further comprising prompting a user to input a value to be used as the predetermined level (see abstract; col.2, lines 42-65 where the assigned confidence rating corresponds to Applicant's predetermined level) .

**As per claims 6, 12, 18 and 24** Joyce (6,519,703 B1) teach the method, system, storage medium including computer executable code of selecting a detecting method as recited in the claims 5, 11, 17 and 23, further comprising receiving the value input by the user and using the value as the predetermined level (see abstract; col.2, lines 42-65 where the assigned confidence rating corresponds to Applicant's predetermined level; and col.5, lines 38-45; col.6, lines 30-65 where the algorithm used are base on the input data that corresponds to Applicant's input value) .

**As per claims 25-28** Joyce (6,519,703 B1) teach a method, system, storage medium and a programmed computer system including computer executable code for selecting a detection method for analyzing computer code for malicious code (see abstract; fig.2 and associated text), comprising: providing a plurality of malicious code detection methods (see abstract; col.2, lines 16-29); determining a degree of accuracy of a result of the analysis (see abstract; col.2) , and repeating the analyzing and determining steps, if the degree of accuracy is below a predetermined level (see abstract; col.2, lines 42-65 where the assigned confidence rating corresponds to Applicant's predetermined level; col.2, lines 53-57 where if it is a poor confidence which corresponds to Applicant's below pre determined level); and outputting a result of the analysis if the probability of accuracy is at or above the predetermined level (see col.2, lines 47-51 where if it is a high confidence which corresponds to Applicant's at or above pre-determined level), also see col.2-6 and col.7, lines 1-5 for more detailed but do not disclose explicitly wherein at least some of the malicious code detection methods require different amounts of time to analyze for malicious code; selecting a fastest one of the malicious code detection methods, analyzing computer code for malicious code using the selected malicious code detection method; selecting a next fastest one of the malicious code detection methods. However AAPA disclose at least some of the malicious code detection methods require different amounts of time to analyze for malicious code; selecting a fastest one of the malicious code detection methods, analyzing computer code for malicious code using the selected malicious code detection method; selecting a next fastest one of the malicious code detection methods (see page 1 and 2 of the specification). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize AAPA's prior art disclosure in Joyce's Heuristic's packet filtering analysis in order to provide different methods based on Heuristic's logic based rules.

**As per claims 29-32** Joyce (6,519,703 B1) teach a method, system, storage medium and a programmed computer system including computer executable code for selecting a detection method for analyzing computer code for malicious code (see abstract; fig.2 and associated text), comprising: providing a plurality of malicious code detection methods (see abstract; col.2, lines 16-29); determining a degree of accuracy of a result of the analysis (see abstract; col.2) , and repeating the analyzing and determining steps, if the degree of accuracy is below a predetermined level (see abstract; col.2, lines 42-65 where the assigned confidence rating corresponds to Applicant's predetermined level; col.2, lines 53-57 where if it is a poor confidence which corresponds to Applicant's below pre determined level); and outputting a result of the analysis if the probability of accuracy is at or above the predetermined level (see col.2, lines 47-51 where if it is a high confidence which corresponds to Applicant's at or above pre-determined level), also see col.2-6 and col.7, lines 1-5 for more detailed but do not disclose explicitly wherein at least some of the malicious code detection methods require different amounts of time to analyze for malicious code; selecting a fastest one of the malicious code detection methods, analyzing computer code for malicious code using the selected malicious code detection method; selecting a next fastest one of the malicious code detection methods. However AAPA disclose at least some of the malicious code detection methods require different amounts of time to analyze for malicious code;

selecting a fastest one of the malicious code detection methods, analyzing computer code for malicious code using the selected malicious code detection method; selecting a next fastest one of the malicious code detection methods (see page 1 and 2 of the specification). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize AAPA's prior art disclosure in Joyce's Heuristic's packet filtering analysis in order to provide different methods based on Heuristic's logic based rules.

## Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (571) 272-3811. The examiner can normally reached on Monday-Thursday (8:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone numbers for the organization where this application or proceeding is assigned as (571) 273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kambiz Zand

07/28/2005
AU 2132